PAT-NO: JP411355858A

DOCUMENT-IDENTIFIER: JP 11355858 A

TITLE: INFORMATION DISTRIBUTION METHOD IN MOBILE COMMUNICATION NETWORK

PUBN-DATE: December 24, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
SAITO, YUKICHI	N/A
KAMISAKA, KYUICHI	N/A
NAKAMURA, HIROSHI	N/A
TAMURA, MOTOI	N/A
AKIYAMA, DAISUKE	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NTT MOBIL COMMUN NETWORK INC	N/A

APPL-NO: JP10163939

APPL-DATE: June 11, 1998

INT-CL (IPC): H04Q007/38, H04L009/08 , H04L009/32

ABSTRACT:

PROBLEM TO BE SOLVED: To encrypt distributed information and to distribute the encrypted information with an encryption method with high security, where management of an encryption key is easy.

SOLUTION: An information server 5 encrypts distributed information by an encryption key and encrypts the encryption key, by using an authentication key different by every mobile station. The encrypted encryption

key and the
distributed information are transferred to a mobile station 1 at the same time
or at different times. The mobile station 1 uses the authentication key
possessed by itself to interpret the encrypted encryption key and uses the
interpreted encryption key to decode the distributed information.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－355858

(43)公開日　平成11年(1999)12月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
9/32			６７５Ａ

審査請求　未請求　請求項の数５　ＯＬ　（全７頁）

(21)出願番号　特願平10－163939

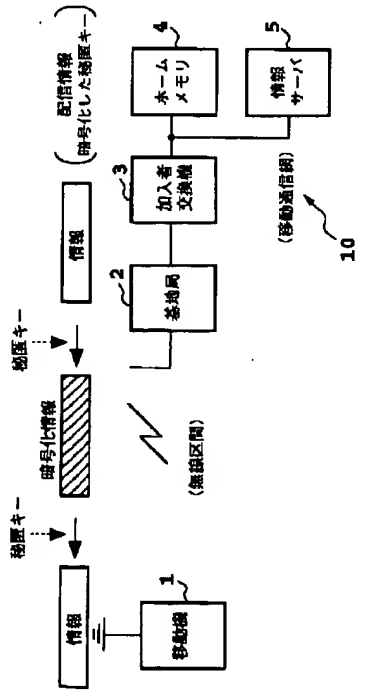
(22)出願日　平成10年(1998)６月11日

(71)出願人　392026693
エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番１号
(72)発明者　斉藤　祐吉
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　上坂　久一
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(72)発明者　中村　寛
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内
(74)代理人　弁理士　谷　義一　（外３名）

最終頁に続く

(54)【発明の名称】　移動通信網における情報配信方法

(57)【要約】
【課題】　秘匿キーの管理が容易で、セキュリティの高い暗号化方法で配信情報を暗号化して配信する。
【解決手段】　情報サーバ５では配信情報を秘匿キーにより暗号化すると共に、秘匿キーを移動機毎に異なる認証キーを使用して暗号化する。暗号化された秘匿キーと配信情報とは同時点あるいは異なる時点で移動機１に転送される。移動機１では自己が保有する認証キーを使用して暗号化された秘匿キーを解読し、次に、解読された秘匿キーを使用して配信情報を解読する。



1

【特許請求の範囲】
【請求項１】　移動通信網内に設置された情報サーバ内に保存された配信情報を暗号化して移動機に配信する移動通信網における情報配信方法において、
前記情報サーバ側では秘匿キーを使用して前記配信情報を暗号化し、
配信対象の移動機の認証に使用する認証キーを使用して前記秘匿キーを暗号化し、
当該暗号化された秘匿キーおよび配信情報を前記配信対象の移動機に送信し、
前記配信対象の移動機では、暗号化されて送信された秘匿キーを自己が保有する認証キーを使用して解読し、
当該解読された秘匿キーを使用して暗号化されて送信された配信情報を解読することを特徴とする移動通信網における情報配信方法。
【請求項２】　請求項１に記載の移動通信網における情報配信方法において、暗号化された前記秘匿キーと暗号化された配信情報を異なる時点で前記情報サーバから前記配信対象の移動機に対して転送することを特徴とする移動通信網における情報配信方法。
【請求項３】　請求項１に記載の移動通信網における情報配信方法において、暗号化された前記秘匿キーと暗号化された配信情報を同時点で前記情報サーバから前記配信対象の移動機に対して転送することを特徴とする移動通信網における情報配信方法。
【請求項４】　請求項１に記載の移動通信網における情報配信方法において、前記秘匿キーを所定タイミングで変更することを特徴とする移動通信網における情報配信方法。
【請求項５】　請求項１に記載の移動通信網における情報配信方法において、前記認証キーおよび前記秘匿キーを記憶するホームメモリを前記移動通信網内に設置し、該ホームメモリから前記情報サーバに対して前記認証キーおよび前記秘匿キーを引き渡すことを特徴とする移動通信網における情報配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、移動通信網において情報の配信のために情報を暗号化する場合の秘匿キーを移動機に設定するための移動通信網における情報配信方法に関する。
【０００２】
【従来の技術】移動通信網においても情報配信サービスが行われている。移動通信網内には情報サーバが設置されており、所定時刻になると、情報サーバ内に記憶されていた配信情報が所定の移動機に対して配信される。このような配信情報は、特定の移動機に対してのみ配信されるためにユーザから情報の秘匿性を求められることが多くなってきている。通信の分野では、通信情報を秘匿するためには暗号化を行っている。暗号化の一般的な方

2

法は情報の送信元は秘匿キー（ある特定の数値等、秘密キーとも呼ばれる）と暗号化のための演算式とを使用して、情報たとえば、文字コード列を他の文字コード列に変換する。暗号化された情報（文字コード列）を受信した送信先では上記秘匿キーと同じ秘匿キーと暗号化とは逆の演算式を使用して、暗号化された情報を解読（復号化とも呼ばれる）する。
【０００３】このような暗号化方法を使用する場合に移動通信では次の点が重要となる。
【０００４】１．情報内容が無線で伝送されるので、盗聴の危険性が大きく、秘匿キーを誰にも知られないようにしておきたい。
【０００５】２．配信情報サービスを受ける移動機は多数なので、移動機毎に秘匿キーを異ならせたい。
【０００６】
【発明が解決しようとする課題】上記第１の点を満足するためには２つの方法が知られている。第１の方法では、秘匿キーをＲＯＭなどに記憶し、人間の指示では上記秘匿キーを読み出せないように秘匿キーをＲＯＭに閉じ込める。この方法は、ＲＯＭを外してＲＯＭリーダにかけるとＲＯＭの記憶内容が読み出されてしまうという欠点と、一度秘匿キーを定めるとその秘匿キーを変更することは困難という欠点がある。
【０００７】第２の方法は、情報送信元が秘匿キーを一定時間毎に変更し、暗号化したときに使用した秘匿キーを暗号文と共に送信元から送信先へ送信する。送信先では受信された秘匿キーで暗号文を解読する。この方法は秘匿キーそのものが盗聴の危険性がある。
【０００８】上記第２の点を満足させるためには、情報の送信元では移動機毎、たとえば、加入者番号毎に秘匿キーを記憶しなければならないので、その情報管理が大変な労力となる。また、秘匿キーを一定時間間隔で変更させたい場合を考慮すると記憶している秘匿キーの変更処理を行うコンピュータシステムに大きな負担がかかる。
【０００９】そこで、本発明は、秘匿キーを使用して配信情報を暗号化して配信する際に、移動通信網側の秘匿キーの管理が容易で、かつ、秘匿キーの変更が可能かつ、秘匿キーおよび配信情報の秘匿性が高い移動通信網における情報配信方法を提供することにある。
【００１０】
【課題を解決するための手段】このような目的を達成するために、請求項１の発明は、移動通信網内に設置された情報サーバ内に保存された配信情報を暗号化して移動機に配信する移動通信網における情報配信方法において、前記情報サーバ側では秘匿キーを使用して前記配信情報を暗号化し、配信対象の移動機の認証に使用する認証キーを使用して前記秘匿キーを暗号化し、当該暗号化された秘匿キーおよび配信情報を前記配信対象の移動機に送信し、前記配信対象の移動機では、暗号化されて送

信された秘匿キーを自己が保有する認証キーを使用して解読し、当該解読された秘匿キーを使用して暗号化されて送信された配信情報を解読することを特徴とする。

【００１１】請求項２の発明は、請求項１に記載の移動通信網における情報配信方法において、暗号化された前記秘匿キーと暗号化された配信情報を異なる時点で前記情報サーバから前記配信対象の移動機に対して転送することを特徴とする。

【００１２】請求項３の発明は、請求項１に記載の移動通信網における情報配信方法において、暗号化された前記秘匿キーと暗号化された配信情報を同時点で前記情報サーバから前記配信対象の移動機に対して転送することを特徴とする。

【００１３】請求項４の発明は、請求項１に記載の移動通信網における情報配信方法において、前記秘匿キーを所定タイミングで変更することを特徴とする。

【００１４】請求項５の発明の発明は、請求項１に記載の移動通信網における情報配信方法において、前記認証キーおよび前記秘匿キーを記憶するホームメモリを前記移動通信網内に設置し、該ホームメモリから前記情報サーバに対して前記認証キーおよび前記秘匿キーを引き渡すことを特徴とする。

【００１５】

【発明の実施の形態】図面を参照して、本発明の実施形態を詳細に説明する。

【００１６】図１に移動通信網におけるシステム構成と情報の流れを示す。図１において、１は移動機であり、配信情報を受信し、移動機１の表示器に配信情報を表示する。移動機１の回路構成は従来と同様のものを使用することができるが、配信情報の解読に係る秘匿キーが暗号化され、その暗号化されている秘匿キーを解読するための処理手順を実行する点が従来と異なる。このような処理手順はたとえば、移動機１内のＲＯＭなどに記憶され、移動機１内のＣＰＵあるいはデジタルプロセッサにより実行される。

【００１７】２は基地局であり、移動機１との間で無線により情報の授受を行う。３は加入者交換機であり、加入者交換機３は基地局２、移動通信網１０内で他の交換機、ホームメモリ４、情報サーバ５との間で情報の授受を行う。

【００１８】基地局３および加入者交換機４は従来と同様とすることができるので、詳細な説明を要しないであろう。４はホームメモリで有り、ホームメモリ４は移動通信網１０内に設置され、移動機１の加入者番号（いわゆる電話番号）および通信パケットアドレス、認証キーおよび秘匿キー、その他、加入者に関する各種の情報を記憶し、管理する。認証キー自体は周知であるが本発明に係るので、簡単に説明しておく。認証キーは、移動機１の認証に使用するコードで有り、通信契約がユーザ（加入者）と移動通信サービス会社との間に結ばれた際に、認証キーが決定される。認証キーは移動機毎に異なり、セキュリティのために、最初の通信時に無線区間を送信するのではなく、オペレータの視点等で直接不揮発性メモリ内に書き込まれ保存される。

【００１９】移動通信網１０側で認証時（位置登録、通信開始に先だって行われる手順）に乱数を発生させ、その乱数を移動機１に転送する。

【００２０】ネットワークはホームメモリに蓄えられている、あるユーザの認証キーを基に、乱数と秘匿キーを使って演算を行う。

【００２１】移動機１も転送されてきた乱数を基に自身が持っている秘匿キーを使って演算を行い、その演算結果を移動通信網１０へ返送する。

【００２２】移動通信網１０では、自身の演算結果と移動機が返送してきた演算結果を照合し、一致していれば認証オーケーで位置登録、通信開始手順を継続する。

【００２３】双方が一致したときに移動機１が移動通信サービス会社と契約したものであると認証される。

【００２４】この認証に使用される認証キーがホームメモリ４に保存されている点に本願発明者は着目し、上述の秘匿キーを上記認証キーを使用して第１の暗号化、転送を行い、秘匿キーを使用して配信情報を第２の暗号化、転送する点が本実施形態の大きな特徴である。このため、秘匿キーはユーザ毎に異なる認証キーにより暗号化されるので、秘匿キーが単一でも暗号化された秘匿キーはユーザ毎に異なったものとなる。したがって、ホームメモリ４は単一の秘匿キーを管理すればよい。本実施形態では、さらにホームメモリ４は一定時間間隔で上記秘匿キーをランダム（乱数的）に変更するがこの変更処理をも簡単に行うことができる。さらに秘匿キーと配信情報は異なるキーで暗号化されるので、単一の暗号化アルゴリズムを使用しても秘匿キーおよび配信情報の秘匿性が高いものとなる。なお、本実施形態では、秘匿キーの暗号化アルゴリズム（演算式）と配信情報の暗号化アルゴリズムは異ならせている。

【００２５】図１に戻り、５は情報サーバであり、配信すべき情報、配信先の移動機に関する加入者番号、移動通信のための通信パケットアドレス等の情報を記憶する。

【００２６】複数の基地局１、複数の加入者交換機１、複数のホームメモリ４、１以上の情報サーバ５は有線の信号線で接続され、移動通信に関する制御情報や通話情報、配信情報を関連者間で転送する。

【００２７】このようなシステム構成において行われる配信情報の配信処理を図２～図５を参照して説明する。図２は配信処理にかかわる通信基本シーケンスの内容を示す。

【００２８】図３は情報サーバ５の配信に係る処理手順を示す。図４はホームメモリ４の配信に係る処理手順を示す。図４は配信情報を受け取る移動機１の処理手順を

示す。

【００２９】情報サーバ５では内部に記憶されている配信スケジュールに従って、現在の時刻に配信すべき配信情報があるか否かを判定する（図３のステップＳ１００）。現在の時刻に配信すべき配信情報がある場合に情報サーバ５は登録されている移動機１に対して、呼び出しを行う。この呼び出しは、通常の通話と同様、加入者番号による呼び出しを行う形態をとってもよいし、配信情報を配信する旨の識別子をもたせた呼びかけを意味する通信パケットを加入者交換機３、基地局１を介して移動機１に送信する形態をとってもよい。この呼び出しを移動機１が受信すると（図５のステップＳ３００）、移動機１では呼び出しに応答し、次に認証要求を待つ（図５のステップＳ３１０→Ｓ３２０）。

【００３０】移動機１からの応答を基地局２、加入者交換機３を介して受けたホームメモリ４では、移動機１に対応する登録の認証キーを加入者交換機３に送信する。加入者交換機３は従来と同様にして移動機１に対して認証要求を基地局２経由で送信する（図４のステップＳ２００→Ｓ２１０）。

【００３１】認証要求を受けた移動機１では内部に記憶してある秘匿キーを使用して演算を行いその演算結果を基地局２に送信する（図５のステップＳ３２０→Ｓ３３０）。本実施形態では加入者交換機３において移動通信網側での演算結果と移動機１側からの演算結果との照合を行う。この照合において、一致の判定、すなわち、認証成功の判定が行われると、移動機１と基地局２との間の無線区間の設定、加入者交換機３、ホームメモリ４、情報サーバ５間の中継区間の設定が行われ、移動機１と情報サーバ５との接続が行われる。以上までの処理手順は従来と同様である。

【００３２】認証キーによる認証後、情報サーバ５はホームメモリ４に対して秘匿キーおよび認証キーの送信要求をホームメモリ４に対して送信し、ホームメモリ４から認証キーおよび秘匿キーを受信する（図３のステップＳ１２０）。情報サーバ５は受信した認証キーを使用して秘匿キーを暗号化する（図３のステップＳ１３０）。暗号化のアルゴリズム自体は本発明を実施する上でのセキュリティの問題から開示できないので、仮の暗号化方法を説明する。一例としては、認証キーの示す数値（たとえば、１０進数で５）と秘匿キーの示す数値（たとえば、１０進法で３）を乗算する。その乗算結果（数値１５）が暗号化された秘匿キーの値となる。異なる移動機１に対してはその認証キーが数値４とすると暗号化された秘匿キーの値は４×３＝１２となり、上述の値１５と互いに異なることに注意されたい。当然のことながら秘匿キーの値３とも異なることは言うまでもない。

【００３３】次に情報サーバ５は秘匿キーを使用して秘匿キーの暗号化方法とは異なる第２の暗号化方法で秘匿キーを暗号化する。送信する配信情報が文字コード列とすると、文字コード列の各文字コードの示す数値に秘匿キーの値（この場合３）を加算して暗号化した文字コード列を作成する（図３のステップＳ１４０）。

【００３４】このようにして第１の暗号化方法により暗号化された秘匿キーおよび第２の暗号化方法により暗号化された配信情報は配信指定された移動機（配信対象の移動機）１に対して配信される（図３のステップＳ１５０）。

【００３５】認証手順終了後、暗号化された秘匿キーおよび配信情報を受信し（図５のステップＳ３４０）、秘匿キーを最初に解読する（図５のステップＳ３５０）。暗号化された秘匿キーの値は１５（５×３）であるので、自己が保存する照合用の認証キー（数値５）を使用して乗算の逆すなわち、暗号化された値１５を照合用の認証キーの値５で除算して秘匿キーの値を取得する。

【００３６】次に移動機１では秘匿キーの値を使用して、受信した配信情報の解読を行う。この例では秘匿キーの加算により暗号化化が行われるので、暗号化された文字コード列の各文字コードの値から秘匿キーの値３を減算して配信情報の復号化を行う（図５のステップＳ３６０）。解読（復号化）された配信情報は移動機１の表示器に表示される（図５のステップＳ３７０）。

【００３７】ホームメモリ４では情報サーバ５の要求に応じて認証キーおよび秘匿キーを送信した後（図４のステップＳ２３０の後）、図４のステップＳ２００→Ｓ２４０→Ｓ２６０の手順を繰り返して、秘匿キーの変更時刻になるのを待つ。たとえば、前回の秘匿キーの変更から１時間が経過し、変更時刻に到達したことをホームメモリ１が検知すると（図４のステップＳ２４０のＹＥＳ判定）、ホームメモリ４はたとえば、乱数器を使用して新規の秘匿キーを発生する。作成された秘匿キーは内部の記憶装置に保存され、次の変更があるまでの間、情報サーバ５側の暗号化のために使用される。以下、一定時刻を経過するごとに秘匿キーは変更される。

【００３８】以上の配信処理では、移動機１側では、暗号化され、時刻によって異なる秘匿キーを受信するので、暗号解読のための演算式（アルゴリズム）は他の移動機１と同じものを使用することができる。また、基地局２と複数の移動機１との間で無線で配信情報が伝送されても、伝送される暗号化された秘匿キーの値は移動機毎に異なるので、たとえ、無線を盗聴しても、その盗聴情報に秘匿キーが含まれることすら識別できないであろう。

【００３９】さらにホームメモリ４では単一の秘匿コードを所定時間毎に（間隔は一定にする必要はない）変更すればよいので、秘匿コードの管理（保存、変更）が非常に容易である。

【００４０】上述の実施形態の他に次の形態を実施できる。

【００４１】１）上述の実施形態では、秘匿キーを変更

しているので、暗号化された秘匿キーと配信情報を異なる暗号方法で暗号化し移動機１に配信しているが、秘匿キーを固定化したい場合には、秘匿キーと配信情報を異なるタイミングで情報サーバから配信するとよい。この場合には、暗号化方法を共通化できる。暗号化された秘匿キーの送信タイミングとしては、移動機１から位置登録要求があった時点や、発信があった時点とすることができる。

【００４２】２）上述の実施形態では、秘匿キーをホームメモリ４が管理し、配信情報を情報サーバ５が管理しているが、秘匿キーを情報サーバ５に管理させてもよい。

【００４３】３）秘匿キーおよび配信情報を暗号化するための暗号化方法は任意の方法を使用することができる。

【００４４】４）上述の実施形態では、移動機１の表示器に配信情報を表示させる形態を説明したが、移動機１に接続された端末、たとえば、電子手帳等やモバイルコンピュータと呼ばれる情報処理装置により配信情報を表示してもよい。

【００４５】５）上述の実施形態では単一種の秘匿コードを使用する形態を説明したが、この秘匿コードは同報通信の様に、配信情報を複数の同報通信者に通信する場合に使用するとよい。情報配信サービス契約者が異なる場合には秘匿コードを異ならせればよいことは言うまでもないであろう。

【００４６】６）配信情報は文字に限らず、イメージ、音声、ＨＴＭＬ言語で記載された文書情報、あるいはこれら情報が混在した情報、端末側で実行するソフトウェアプログラム（アプリケーションプログラムとも呼ばれる）等、各種の情報を取り扱うことができる。

【００４７】

【発明の効果】以上、説明したように、請求項１の発明では、配信情報の暗号化に使用した秘匿キーをも暗号化して移動機側に転送するので、移動機側では秘匿キーを保持する必要がなく、秘匿キーを配信情報の送信側で自由に変えることができる。さらに秘匿キーを認証キーを使用して暗号化することにより暗号化された秘匿キーの内容は移動機毎に異なるので、たとえ、暗号化された秘匿キーが盗聴されても、秘匿キーそのものの安全性が図られる。さらには秘匿キー自体は認証番号毎、すなわち、移動機毎に設定する必要はないので、秘匿キーの種類を少なくでき、秘匿キーの管理が容易となる。

【００４８】請求項２の発明では、暗号化された秘匿キーと配信情報の送信タイミングを異ならせることにより、共通の暗号化方法で暗号化を行っても、その秘匿性が損なわれることはない。

【００４９】請求項３の発明では、暗号化された秘匿キーと配信情報を同時点で送信することにより秘匿キーを変更しても受信側の移動機では受信の秘匿キーを使用すればよく、配信情報の送信タイミングあるいは秘匿情報の更新タイミングに制約を与えることはない。

【００５０】請求項４の発明では、秘匿キーを変更することにより、秘匿キー、ひいては配信情報の安全性、秘匿性が高まる。

【００５１】請求項５の発明では、認証キーおよび秘匿キー等の秘匿性に係る情報を配信情報を記憶しておく情報サーバとは別のホームメモリに記憶しておくことで、配信情報および上記認証キーおよび秘匿キーの暗号解読に係るキーの全部を入手することは困難となる。

【図面の簡単な説明】

【図１】本発明実施形態の配信処理手順を示す説明図である。

【図２】本発明実施形態のシステム構成および情報の流れを示す構成図である。

【図３】図１の情報サーバ５の処理手順を示すフローチャートである。

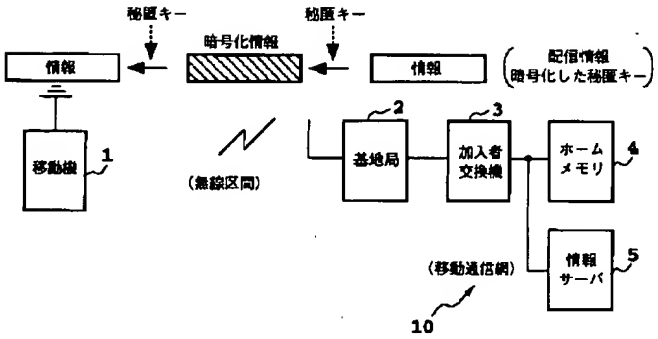
【図４】図１のホームメモリの処理手順を示すフローチャートである。

【図５】図１の移動機の処理手順を示すフローチャートである。

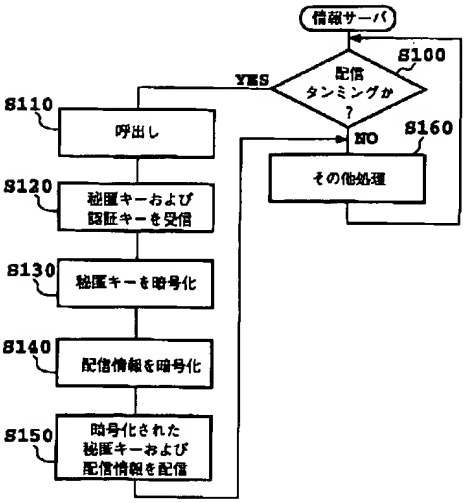
【符号の説明】

１　移動機
２　基地局
３　加入者交換機
４　ホームメモリ
５　情報サーバ

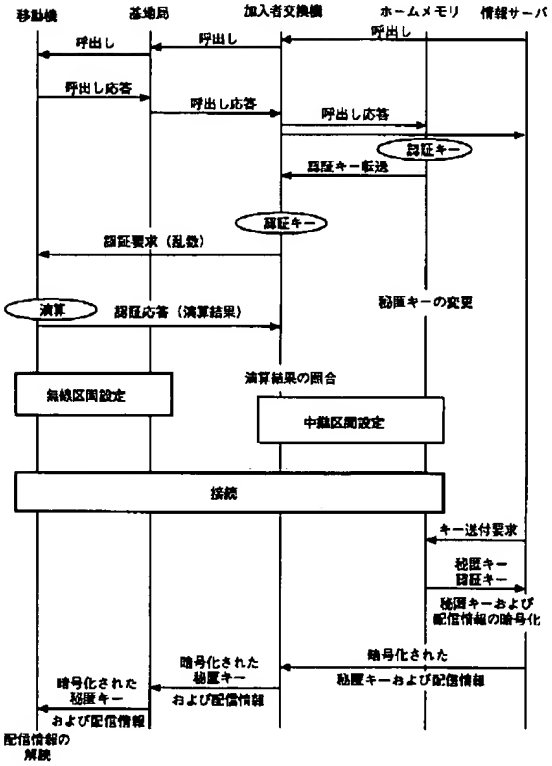
【図1】


秘匿キー
秘匿キー
暗号化情報
情報
情報
配信情報
暗号化した秘匿キー
移動機
1
（無線区間）
2
基地局
3
加入者交換機
ホームメモリ
4
情報サーバ
5
（移動通信網）
10

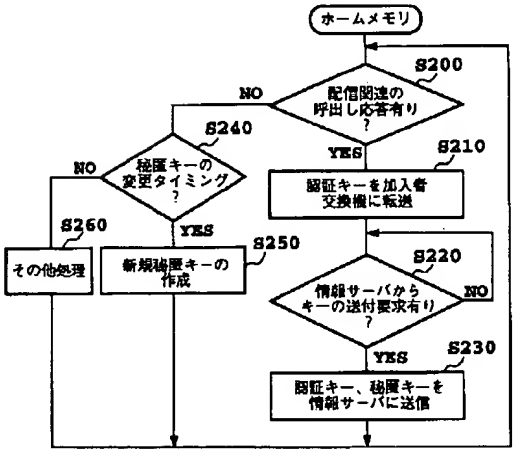
【図3】


情報サーバ
S100
配信タイミングか？
YES
NO
S110
呼出し
S120
秘匿キーおよび認証キーを受信
S130
秘匿キーを暗号化
S140
配信情報を暗号化
S150
暗号化された秘匿キーおよび配信情報を配信
S160
その他処理

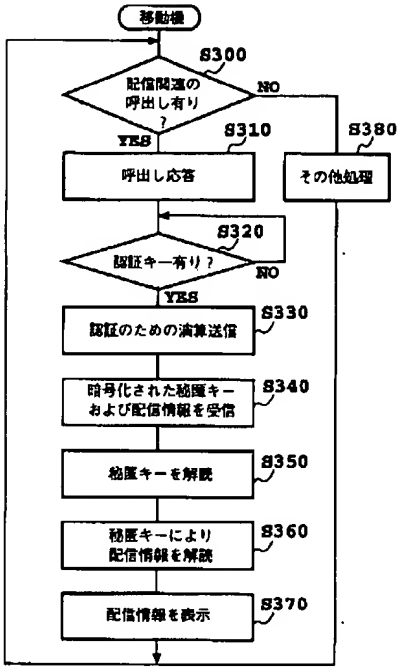
【図2】


移動機
基地局
加入者交換機
ホームメモリ
情報サーバ
呼出し
呼出し
呼出し
呼出し応答
呼出し応答
呼出し応答
認証キー
認証キー転送
認証キー
認証要求（乱数）
演算
認証応答（演算結果）
秘匿キーの変更
演算結果の照合
無線区間設定
中継区間設定
接続
キー送付要求
秘匿キー
認証キー
秘匿キーおよび配信情報の暗号化
暗号化された秘匿キーおよび配信情報
暗号化された秘匿キーおよび配信情報
暗号化された秘匿キーおよび配信情報
配信情報の解読

【図4】


ホームメモリ
S200
配信関連の呼出し応答有り？
NO
YES
S240
秘匿キーの変更タイミング？
NO
YES
S260
その他処理
S250
新規秘匿キーの作成
S210
認証キーを加入者交換機に転送
S220
情報サーバからキーの送付要求有り？
NO
YES
S230
認証キー、秘匿キーを情報サーバに送信

【図５】



フロントページの続き

(72)発明者　田村　基
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内

(72)発明者　秋山　大介
東京都港区虎ノ門二丁目10番１号　エヌ・ティ・ティ移動通信網株式会社内